OPINION OF ADVOCATE GENERAL
JÄÄSKINEN
delivered on 25 June 2013 (1)

Case C-131/12

Google Spain SL
Google Inc.
v
Agencia Española de Protección de Datos (AEPD)
Mario Costeja González

(Reference for a preliminary ruling from the Audiencia Nacional (Spain))

(World Wide Web – Personal data – Internet search engine – Data Protection Directive 95/46 – Interpretation of Articles 2(b) and 2(d), 4(1)(a) and 4(1)(c), 12(b) and 14(a) – Territorial scope of application – Concept of an establishment on the territory of a Member State – Scope of application ratione materiae – Concept of processing of personal data – Concept of a controller of processing of personal data – Right to erasure and blocking of data – 'Right to be forgotten' – Charter of Fundamental Rights of the European Union – Articles 7, 8, 11 and 16)

I – Introduction

1. In 1890, in their seminal Harvard Law Review article 'The Right to Privacy', (2) Samuel D. Warren and Louis D. Brandeis lamented that '[r]ecent inventions and business methods' such as '[i]nstantenous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life'. In the same article they referred 'to the next step which must be taken for the protection of the person.'

2. Nowadays, protecting personal data and privacy of individuals has become increasingly important. Any content including personal data, be it in the form of texts or audiovisual materials, can instantly and permanently be made accessible in digital format world wide. The internet has revolutionised our lives by removing technical and institutional barriers to dissemination and reception of information, and has created a platform for various information society services. These benefit consumers, undertakings and society at large. This has given rise to unprecedented circumstances in which a balance has to be struck between various fundamental rights, such as freedom of expression, freedom of information and freedom to conduct a business, on one hand, and protection of personal data and the privacy of individuals, on the other.

3. In the context of the internet, three situations should be distinguished that relate to personal

data. The first is the publishing of elements of personal data on any web page on the internet (3) (the 'source web page'). (4) The second is the case where an internet search engine provides search results that direct the internet user to the source web page. The third, more invisible operation occurs when an internet user performs a search using an internet search engine, and some of his personal data, such as the IP address from which the search is made, are automatically transferred to the internet search engine service provider. (5)

4. As regards the first situation, the Court has already held in *Lindqvist* that Directive 95/46/EC (6) (hereinafter 'the Data Protection Directive' or 'the Directive') applies to this situation. The third situation is not at issue in the present proceedings, and there are ongoing administrative procedures initiated by national data protection authorities to clarify the scope of application of the EU data protection rules to the users of internet search engines. (7)

5. The order for reference in this case relates to the second situation. It has been made by the Audiencia Nacional (the National High Court of Spain) in the course of proceedings between Google Spain SL and Google Inc. (individually or jointly 'Google') on the one side and the Agencia Española de Protección de Datos ('the AEPD') and Mr Mario Costeja González ('the data subject') on the other side. The proceedings concern the application of the Data Protection Directive to an internet search engine that Google operates as service provider. In the national proceedings it is undisputed that some personal data regarding the data subject have been published by a Spanish newspaper, in two of its printed issues in 1998, both of which were republished at a later date in its electronic version made available on the internet. The data subject now thinks that this information should no longer be displayed in the search results presented by the internet search engine operated by Google, when a search is made of his name and surnames.

6. The questions referred to the Court fall into three categories. (8) The first group of questions relates to *territorial scope of application* of EU data protection rules. The second group addresses the issues relating to the legal position of an internet search engine service provider (9) in the light of the Directive, especially in terms of its *scope of application ratione materiae*. Finally, the third question concerns the so-called *right to be forgotten* and the issue of whether data subjects can request that some or all search results concerning them are no longer accessible through search engine. All of these questions, which also raise important points of fundamental rights protection, are new to the Court.

7. This appears to be the first case in which the Court is called upon to interpret the Directive in the context internet search engines; an issue that is seemingly topical for national data protection authorities and Member State courts. Indeed, the referring court has indiciated that it has several similar cases pending before it.

8. The most important previous case of this Court in which data protection issues and the internet have been addressed was *Lindqvist* (10). However, in that case internet search engines were not involved. The Directive itself has been interpreted in a number of cases. Of these *Österreichischer Rundfunk,* (11)*Satakunnan Markkinapörssi and Satamedia* (12) and *Volker und Markus Schecke and Eifert* (13) are particularily relevant. The role of internet search engines in relation to intellectual property rights and jurisdiction of courts has also been addressed in the case-law of the Court in *Google France and Google*, *Portakabin*, *L'Oréal and Others*, *Interflora and Interflora British Unit* and *Wintersteiger*. (14)

9. Since the adoption of the Directive, a provision on protection of personal data has been included in Article 16 TFEU and in Article 8 of the Charter of Fundamental Rights of the European Union ('the Charter'). Moreover, in 2012, the Commission made a Proposal for a General Data Protection Regulation, (15) with a view to replacing the Directive. However, the dispute to hand has

to be decided on the basis of existing law.

10. The present preliminary reference is affected by the fact that when the Commission proposal for the Directive was made in 1990, the internet in the present sense of the World Wide Web, did not exist, and nor were there any search engines. At the time the Directive was adopted in 1995 the internet had barely begun and the first rudimentary search engines started to appear, but nobody could foresee how profoundly it would revolutionise the world. Nowadays almost anyone with a smartphone or a computer could be considered to be engaged in activities on the internet to which the Directive could potentially apply.

II – Legal framework

A – *The Data Protection Directive*

11. Article 1 of the Directive obliges Member States to protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data, in accordance with the provisions of the Directive.

12. Article 2 defines, inter alia, the notions of ‘personal data’ and ‘data subject’, ‘processing of personal data’, ‘controller’ and ‘third party’.

13. According to Article 3, the Directive is to apply to the processing of personal data wholly or partly by automatic means, and in certain situations to the processing otherwise than by automatic means.

14. Pursuant to Article 4(1), a Member State is to apply the national provisions it adopts pursuant to the Directive to the processing of personal data where there is an establishment of the controller on its territory, or in cases where the controller is not established in the Union, if he makes use of equipment situated on the territory of the Member State for the purposes of processing personal data.

15. Article 12 of the Directive provides data subjects ‘a right of access’ to personal data processed by the controller and Article 14 a ‘right to object’ to the processing of personal data in certain situations.

16. Article 29 of the Directive sets up an independent advisory working party consisting, among others, of data protection authorities of the Member States (‘the Article 29 Working Party’).

B – *National law*

17. Organic Law No 15/1999 on data protection has transposed the Directive in Spanish law. (16)

III – Facts and questions referred for a preliminary ruling

18. In early 1998, a newspaper widely circulated in Spain published in its printed edition two announcements concerning a real-estate auction connected with attachment proceedings prompted by social security debts. The data subject was mentioned as the owner. At a later date an electronic version of the newspaper was made available online by its publisher.

19. In November 2009, the data subject contacted the publisher of the newspaper asserting that, when his name and surnames were entered in the Google search engine, a reference appeared to pages of the newspaper with the announcements concerning the real-estate auction. He argued that the attachment proceedings relating to his social security debts had been concluded and resolved

many years earlier and were now of no relevance. The publisher replied to him saying that erasure of his data was not appropriate, given that the publication was effected by order of the Ministry of Labour and Social Affairs.

20. In February 2010, the data subject contacted Google Spain and requested that the search results should not show any links to the newspaper when his name and surnames were entered in the Google search engine. Google Spain forwarded the request to Google Inc., whose registered office is in California, United States, taking the view that the latter was the undertaking providing the internet search service.

21. Thereafter the data subject lodged a complaint with the AEPD asking that the publisher be required to remove or rectify the publication so that his personal data did not appear or else should use the tools made available by search engines to protect his personal data. He also asserted that Google Spain or Google Inc. should be required to remove or conceal his data so that they ceased to be included in the search results and reveal links to the newspaper.

22. By a decision on 30 July 2010, the Director of the AEPD upheld the complaint made by the data subject against Google Spain and Google Inc., calling on them to take the measures necessary to withdraw the data from their index and to render future access to them impossible but rejected the complaint against the publisher. This was so because publication of the data in the press was legally justified. Google Spain and Google Inc. have brought two appeals before the referring court, seeking annulment of the AEPD decision.

23. The national court has stayed the proceedings and referred the following questions to the Court for a preliminary ruling:

‘1. With regard to the territorial application of [the Directive] and, consequently, of the Spanish data protection legislation:

1.1. must it be considered that an “establishment”, within the meaning of Article 4(1)(a) of [the Directive], exists when any one or more of the following circumstances arise:

– when the undertaking providing the search engine sets up in a Member State an office or subsidiary for the purpose of promoting and selling advertising space on the search engine, which orientates its activity towards the inhabitants of that State,

or

– when the parent company designates a subsidiary located in that Member State as its representative and controller for two specific filing systems which relate to the data of customers who have contracted for advertising with that undertaking,

or

– when the office or subsidiary established in a Member State forwards to the parent company, located outside the European Union, requests and requirements addressed to it both by data subjects and by the authorities with responsibility for ensuring observation of the right to data protection, even where such collaboration is engaged in voluntarily?

1.2. Must Article 4(1)(c) of [the Directive] be interpreted as meaning that there is “use of equipment … situated on the territory of that Member State”

when a search engine uses crawlers or robots to locate and index information contained in web

pages located on servers in that Member State

or

when it uses a domain name pertaining to a Member State and arranges for searches and the results thereof to be based on the language of that Member State?

1.3. Is it possible to regard as a use of equipment, in the terms of Article 4(1)(c) of [the Directive], the temporary storage of the information indexed by internet search engines? If the answer to that question is affirmative, can it be considered that that connecting factor is present when the undertaking refuses to disclose the place where it stores those indexes, invoking reasons of competition?

1.4. Regardless of the answers to the foregoing questions and particularly in the event that the [Court] considers that the connecting factors referred to in Article 4 of the Directive are not present:

must [the Directive] be applied, in the light of Article 8 of the [Charter], in the Member State where the centre of gravity of the conflict is located and more effective protection of the rights of European Union citizens is possible?

2. As regards the activity of search engines as providers of content in relation to [the Directive]:

2.1. in relation to the activity of the search engine of the 'Google' undertaking on the internet, as a provider of content, consisting in locating information published or included on the net by third parties, indexing it automatically, storing it temporarily and finally making it available to internet users according to a particular order of preference, when that information contains personal data of third parties,

must an activity like the one described be interpreted as falling within the concept of "processing of … data" used in Article 2(b) of [the Directive]?

2.2. If the answer to the foregoing question is affirmative, and once again in relation to an activity like the one described: must Article 2(d) of the Directive be interpreted as meaning that the undertaking managing the "Google" search engine is to be regarded as the 'controller' of the personal data contained in the web pages that it indexes?

2.3. In the event that the answer to the foregoing question is affirmative, may the national data-control authority (in this case the [AEPD]), protecting the rights embodied in Articles 12(b) and 14(a) of [the Directive], directly impose on the search engine of the "Google" undertaking a requirement that it withdraw from its indexes an item of information published by third parties, without addressing itself in advance or simultaneously to the owner of the web page on which that information is located?

2.4. In the event that the answer to the foregoing question is affirmative, would the obligation of search engines to protect those rights be excluded when the information that contains the personal data has been lawfully published by third parties and is kept on the web page from which it originates?

3. Regarding the scope of the right of erasure and/or the right to object, in relation to the "derecho al olvido" (the "right to be forgotten"), the following question is asked:

3.1. must it be considered that the rights to erasure and blocking of data, provided for in Article 12(b), and the right to object, provided for by Article 14(a), of [the Directive], extend to enabling

the data subject to address himself to search engines in order to prevent indexing of the information relating to him personally, published on third parties' web pages, invoking his wish that such information should not be known to internet users when he considers that it might be prejudicial to him or he wishes it to be consigned to oblivion, even though the information in question has been lawfully published by third parties?'

24. Written observations were submitted by Google, the Governments of Spain, Greece, Italy, Austria and Poland, and European Commission. With the exception of the Polish Government, all of them attended the hearing on 26 February 2013, as did the representative of the data subject, and presented oral argument.

IV – Preliminary observations

A – *Introductory remarks*

25. The key issue in the present case is how the role of internet search engine service providers should be interpreted in the light of the existing EU legal instruments relating to data protection, and in particular the Directive. Therefore it is instructive to start with some observations relating to the development of data protection, the internet and internet search engines.

26. At the time when the Directive was negotiated and adopted in 1995 (17), it was given a wide scope of application *ratione materiae*. This was done in order to catch up with technological developments relating to data processing by controllers that was more decentralised than filing systems based on traditional centralised data banks, and which also covered new types of personal data like images and processing techniques such as free text searches. (18)

27. In 1995, generalised access to the internet was a new phenomenon. Today, after almost two decades, the amount of digitalised content available online has exploded. It can be easily accessed, consulted and disseminated through social media, as well as downloaded to various devices, such as tablet computers, smartphones and laptop computers. However, it is clear that the development of the internet into a comprehensive global stock of information which is universally accessible and searchable was not foreseen by the Community legislator.

28. At the heart of the present preliminary reference is the fact that the internet magnifies and facilitates in an unprecended manner the dissemination of information. (19) Similarly, as the invention of printing in the 15th century enabled reproduction of an unlimited number of copies that previously needed to be written by hand, uploading of material on to the internet enables mass access to information which earlier could perhaps only be found after painstaking searches, and at limited physical locations. Universal access to information on the internet is possible everywhere, with the exception of those countries where the authorities have limited, by various technical means (such as electronic firewalls), access to the internet or where the access to telecommunications is controlled or scarce.

29. Due to these developments, the potential scope of application of the Directive in the modern world has become be surprisingly wide. Let us think of a European law professor who has downloaded, from the Court's website, the essential case-law of the Court to his laptop computer. In terms of the Directive, the professor could be considered to be a 'controller' of personal data originating from a third party. The professor has files containing personal data that are processed automatically for search and consultation within the context of activities that are not purely personal or household related. In fact, anyone today reading a newspaper on a tablet computer or following social media on a smartphone appears to be engaged in processing of personal data with automatic means, and could potentially fall within the scope of application of the Directive to the extent this

takes place outside his purely private capacity. (20) In addition, the wide interpretation given by the Court to the fundamental right to private life in a data protection context seems to expose any human communication by electronic means to the scrutiny by reference to this right.

30. In the current setting, the broad definitions of personal data, processing of personal data and controller are likely to cover an unprecedently wide range of new factual situations due to technological development. This is so because many, if not most, websites and files that are accessible through them include personal data, such as names of living natural persons. This obliges the Court to apply a rule of reason, in other words, the principle of proportionality, in interpreting the scope of the Directive in order to avoid unreasonable and excessive legal consequences. This moderate approach was applied by the Court already in *Lindqvist*, where it rejected an interpretation which could have lead to an unreasonably wide scope of application of Article 25 of the Directive on transfer of personal data to third countries in the context of the internet. (21)

31. Hence, in the present case it will be necessary to strike a correct, reasonable and proportionate balance between the protection of personal data, the coherent interpretation of the objectives of the information society and legitimate interests of economic operators and internet users at large. Albeit the Directive has not been amended since its adoption in 1995, its application to novel situations has been unavoidable. It is a complex area where law and new technology meet. The opinions adopted by the Article 29 Working Party provide very helpful analysis in this respect. (22)

B – *Internet search engines and data protection*

32. When analysing the legal position of an internet search engine in relation to the data protection rules, the following elements should be noted. (23)

33. First, in its basic form, an internet search engine does not in principle create new autonomous content. In its simplest form, it only indicates where already existing content, made available by third parties on the internet, can be found by giving a hyperlink to the website containing the search terms.

34. Second, the search results displayed by an internet search engine are not based on an instant search of the whole World Wide Web, but they are gathered from content that the internet search engine has previously processed. This means that the internet search engine has retrieved contents from existing websites and copied, analysed and indexed that content on its own devices. This retrieved content contains personal data if any of the source web pages do.

35. Third, to make the results more user-friendly, internet search engines often display additional content alongside the link to the original website. There can be text extracts, audiovisual content or even snapshots of the source web pages. This preview information can be at least in part retrieved from the devices of the internet search engine service provider, and not instantly from the original website. This means that the service provider actually holds the information so displayed.

C – *Regulation of internet search engines*

36. The European Union has attached great importance to the development of the information society. In this context, the role of information society intermediaries has also been addressed. Such intermediaries act as bridge builders between content providers and internet users. The specific role of intermediaries has been recognised, for example, in the Directive (recital 47 in the preamble thereto), in the ecommerce Directive 2000/31 (24) (Article 21(2) and recital 18 in the preamble thereto) as well as in Opinion 1/2008 of the Article 29 Working Party. The role of internet service providers has been considered as crucial for the information society, and their liability for the

third-party content they transfer and/or store has been limited in order to facilitate their legitimate activities.

37. The role and legal position of internet search engine service providers has not been expressly regulated in EU legislation. As such 'information location tool services' are 'provided at a distance, by electronic means and at the individual request of a recipient of services', and amount thus to an information society service consisting of provision of tools that allow for search, access and retrieval of data. However, internet search engine service providers like Google who do not provide their service in return for remuneration from the internet users, appear to fall in that capacity outside the scope of application of ecommerce Directive 2000/31. (25)

38. Despite this, it is necessary to analyse their position vis-à-vis the legal principles underpinning the limitations on the liability of internet service providers. In other words, to what extent are activities performed by an internet search engine service provider, from the point of view of liability principles, analogous to the services enumerated in the ecommerce Directive 2000/31 (transfer, mere caching, hosting) or transmission service mentioned in recital 47 in the preamble to the Directive, and to what extent does the internet search engine service provider act as content provider in its own right.

D – *The role and liability of source web page publishers*

39. The Court found in *Lindqvist* that 'the operation of loading personal data on an internet page must be considered to be [processing of personal data]'. (26) Moreover, 'placing information on an internet page entails, under current technical and computer procedures, the operation of loading that page onto a server and the operations necessary to make that page accessible to people who are connected to the internet. Such operations are performed, at least in part, automatically.' The Court concluded that 'the act of referring, on an internet page, to various persons and identifying them by name or by other means' 'constitutes "the processing of personal data" wholly or partly by automatic means within the meaning of Article 3(1) of [the Directive]'.

40. It follows from the above findings in *Lindqvist* that the publisher of source web pages containing personal data is a controller of processing of personal data within the meaning of the Directive. As such the publisher is bound by all the obligations the Directive imposes on the controllers.

41. Source web pages are kept on host servers connected to internet. The publisher of source web pages can make use of 'exclusion codes' (27) for the operation of the internet search engines. Exclusion codes advise search engines not to index or to store a source web page or to display it within the search results. (28) Their use indicates that the publisher does not want certain information on the source web page to be retrieved for dissemination through search engines.

42. Therefore, technically, the publisher has the possibility to include in his web pages exclusion codes restricting indexing and archiving of the page, and thereby enhancing the protection of personal data. In the extreme, the publisher can withdraw the page from the host server, republish it without the objectionable personal data, and require updating of the page in the cache memories of search engines.

43. Hence, the person who publishes the content on the source web page, is in his capacity of controller liable for the personal data published on the page, and that person has various means for fulfilling his obligations in this respect. This channelling of legal liability is in line with the established principles of publisher liability in the context of traditional media. (29)

44. This liability of publisher does not, however, guarantee that the data protection problems

may be dealt with conclusively only by recourse to the controllers of the source web pages. As the referring court has pointed out, it is possible that the same personal data has been published on innumerable pages, which would make tracing and contacting all relevant publishers difficult or even impossible. Moreover, the publisher might reside in a third country, and the web pages concerned could fall outside the scope of application of EU data protection rules. There might also be legal impediments such as in the present case where the retaining of the original publication on the internet has been considered to be lawful.

45. In fact, universal accessibility of information on the internet relies on internet search engines, because finding relevant information without them would be too complicated and difficult, and would produce limited results. As the referring court rightly observes, acquiring information about announcements on the forced sale of the data subject's property would previously have required a visit to the archives of the newspaper. Now this information can be acquired by typing his name into an internet search engine and this makes the dissemination of such data considerably more efficient, and at the same time, more disturbing for the data subject. Internet search engines may be used for extensive profiling of individuals by searching and collecting their personal data. Yet the fear relating to the profiling of individuals was the inspiration for the development of modern data protection legislation. (30)

46. For these reasons, it is important to examine the liability of internet search engine service providers in respect of personal data published on third-party source web pages which are accessible through their search engines. In other words, the Court is here faced with the issue of 'secondary liability' of this category of information society service providers analogous to that it has dealt with in its case-law on trademarks and electronic marketplaces. (31)

E – *Activities of an internet search engine service provider*

47. An internet search engine service provider may have various types of activities. The nature and assessment of those activities from the data protection point of view may be different.

48. An internet search engine service provider may automatically acquire personal data relating to its users, (32) that is, persons who enter search terms into the search engine. This automatically transmitted data can include their IP address, user preferences (language, etc.), and of course the search terms themselves which in the case of so-called vanity searches (that is, searches made by a user with his own name) easily reveal the identity of users. Moreover, as regards persons who have user accounts and who have thus registered themselves, their personal data such as names, e-mail addresses and telephone numbers, almost invariably end up in the hands of the internet search engine service provider.

49. The revenue of internet search engine service providers does not come from the users who enter the search terms in the search engine, but from the advertisers who buy search terms as keywords so that their advertisement is displayed simultaneously with the search results of using that keyword. (33) It is obvious that personal data relating to advertising customers comes into the possession of the service provider.

50. However, the present preliminary ruling concerns Google acting as a simple internet search engine service provider in relation to data, including personal data, published on the internet in third-party source web pages and processed and indexed by Google's search engine. Hence, the problems of the users and advertising customers, to whose data the Directive is undoubtedly applicable with respect to their relationship with Google, do not affect the analysis of the second group of preliminary questions. However, concerning the jurisdictional issues under the first group of preliminary questions these customer groups may be relevant.

V – First group of questions relating to territorial scope of application of the Directive

A – *Introduction*

51. The first group of preliminary questions concerns the interpretation of Article 4 of the Directive, as regards the criteria determining the territorial scope of application of the national implementing legislation.

52. The referring court has divided its preliminary questions with regard to the territorial application of the Spanish data protection legislation into four sub-questions. The first sub-question relates to the concept of an 'establishment', within the meaning of Article 4(1)(a) of the Directive and the second to the circumstances where there is 'use of equipment … situated on the territory of that Member State' within the meaning of Article 4(1)(c) thereof. The third sub-question asks if it is possible to regard, as use of equipment, the temporary storage of the information indexed by internet search engines, and if the answer to that question is affirmative, whether the presence of this connecting factor may be presumed where the undertaking refuses to disclose the place where it stores those indexes. The fourth sub-question asks whether the legislation implementing the Directive must be applied, in the light of Article 8 of the Charter, in the Member State where the centre of gravity of the dispute is situated and where more effective protection of the rights of European Union citizens is possible.

53. I shall first address the last sub-question, which the national court has posed 'regardless of the answers to the foregoing questions and particularly in the event that [the Court] considers that the connecting factors referred to in Article 4(1) of the Directive are not present'.

B – *The geographical centre of gravity of the dispute in itself is not sufficient to render the Directive applicable*

54. According to Article 51(2) thereof, the Charter does not extend the field of application of European Union law beyond the powers of the Union or establish any new power or task for the Union, or modify powers and tasks as defined in the Treaties. (34) This principle also applies to Article 8 of the Charter on protection of personal data. Hence, the interpretation of the Directive in accordance with the Charter cannot add any new elements that might give rise to the territorial applicability of the national legislation implementing the Directive to those laid down in Article 4(1) of the Directive. Article 8 of the Charter must, of course, be taken into account in the interpretation of the concepts used in Article 4(1) of the Directive, but the points of attachment defined by the EU legislator cannot be supplemented with an entirely new criterion by reference to that fundamental right. (35)

55. The Article 29 Working Party rightly emphasised that the territorial scope of application of the Directive and the national implementing legislation is triggered either by the location of the establishment of the controller, or the location of the means or equipment being used when the controller is established outside the EEA. Nationality or place of habitual residence of data subjects is not decisive, nor is the physical location of the personal data. (36)

56. The Article 29 Working Party has proposed that in future legislation relevant targeting of individuals could be taken into account in relation to controllers not established in the EU. (37) In the Commission Proposal for a General Data Protection Regulation (2012) (38) the offering of goods or services to data subjects residing in the European Union would be a factor making EU data protection law applicable to third country controllers. Such an approach, attaching the territorial applicability of EU legislation to the targeted public, is consistent with the Court's case-law on the applicability of the ecommerce Directive 2000/31, (39) Regulation No 44/2001, (40) and Directive

2001/29 (41) to cross-border situations.

57. By contrast, the criterion of a targeted public, in the present case Spanish users of Google's internet search engine, in whose eyes the data subject's reputation may have been harmed as a result of the disputed announcements, does not seem to be a factor triggering the territorial applicability of the Directive and its national implementation legislation.

58. Therefore, the centre of gravity of the dispute in Spain cannot be added to the criteria set out in Article 4(1) of the Directive which, in my opinion, fully harmonises the territorial scope of application of Member States' data protection laws. This applies irrespective of whether such a centre of gravity is the nationality or residence of the data subject concerned, the location of the disputed personal data in the newspaper's website, or the fact that Google's Spanish website especially targeted the Spanish public. (42)

59. For these reasons I propose that, if the Court finds it necessary to answer that question, it should answer the fourth sub-question in the negative.

C – *The applicability of the criterion of 'establishment in the EU' to a third country internet search engine service provider*

60. According to Article 4(1) of the Directive, the primary factor that gives rise to the territorial applicability of the national data protection legislation is the processing of personal data carried out in the context of the activities of an establishment of the controller on the territory of the Member State. Further, when a controller is not established on EU territory but uses means or equipment (43) situated on the territory of the Member State for processing of personal data, the legislation of that Member State applies unless such equipment or means is used only for purposes of transit through the territory of the EU.

61. As noted above, the Directive and Article 4 thereof were adopted before the large-scale provision of on-line services on the internet started. Moreover, in this respect, its wording is not consistent and is incomplete. (44) It is no wonder that data protection experts have had considerable difficulties in interpreting it in relation to the internet. The facts of the present case illustrate these problems.

62. Google Inc. is a Californian firm with subsidiaries in various EU Member States. Its European operations are to a certain extent coordinated by its Irish subsidiary. It currently has data centres at least in Belgium and Finland. Information on the exact geographical location of the functions relating to its search engine is not made public. Google claims that no processing of personal data relating to its search engine takes place in Spain. Google Spain acts as commercial representative of Google for its advertising functions. In this capacity is has taken responsibility for the processing of personal data relating to its Spanish advertising customers. Google denies that its search engine performs any operations on the host servers of the source web pages, or that it collects information by means of cookies of non registered users of its search engine.

63. In this factual context the wording of Article 4(1) of the Directive is not very helpful. Google has several establishments on EU territory. This fact would, according to a literal interpretation, exclude the applicability of the equipment condition laid down in Article 4(1)(c) of the Directive. On the other hand, it is not clear to what extent and where processing of personal data of EU resident data subjects takes place in the context of its EU subsidiaries.

64. In my opinion the Court should approach the question of territorial applicability from the perspective of the business model of internet search engine service providers. This, as I have mentioned, normally relies on *keyword advertising* which is the source of income and, as such, the

economic *raison d'être* for the provision of a free information location tool in the form of a search engine. The entity in charge of keyword advertising (called 'referencing service provider' in the Court's case-law (45)) is linked to the internet search engine. This entity needs presence on national advertising markets. For this reason Google has established subsidiaries in many Member States which clearly constitute establishments within the meaning of Article 4(1)(a) of the Directive. It also provides national web domains such as google.es or google.fi. The activity of the search engine takes this national diversification into account in various ways relating to the display of the search results because the normal financing model of keyword advertising follows the pay-per-click principle. (46)

65. For these reasons I would adhere to the Article 29 Working Party's conclusion to the effect that the business model of an internet search engine service provider must be taken into account in the sense that its establishment plays a relevant role in the processing of personal data if it is linked to a service involved in selling targeted advertisement to inhabitants of that Member State. (47)

66. Moreover, even if Article 4 of the Directive is based on a single concept of controller as regards its substantive provisions, I think that for the purposes of deciding on the preliminary issue of territorial applicability, an economic operator must be considered as a single unit, and thus, at this stage of analysis, not be dissected on the basis of its individual activities relating to processing of personal data or different groups of data subjects to which its activities relate.

67. In conclusion, processing of personal data takes place within the context of a controller's establishment if that establishment acts as the bridge for the referencing service to the advertising market of that Member State, even if the technical data processing operations are situated in other Member States or third countries.

68. For this reason, I propose that the Court should answer the first group of preliminary questions in the sense that processing of personal data is carried out in the context of the activities of an 'establishment' of the controller within the meaning of Article 4(1)(a) of the Directive when the undertaking providing the search engine sets up in a Member State for the purpose of promoting and selling advertising space on the search engine, an office or subsidiary which orientates its activity towards the inhabitants of that State.

VI – Second group of questions relating to scope of application *ratione materiae* of the Directive

69. The second group of questions pertains to the legal position of an internet search engine service provider offering access to an internet search engine in the light of the provisions of the Directive. The national court has formulated them as concerning the notions of 'processing' of personal data (question 2.1), and 'controller' (question 2.2.), the competences of the national data protection authority to give orders directly to the internet search engine service provider (question 2.3) and the possible exclusion of protection of personal data by the internet search engine service provider concerning information lawfully published by third parties on the internet (question 2.4). These last two sub-questions are relevant only if the internet search engine service provider can be considered as processing personal data on third-party source web pages and as being the controller thereof.

A – *Processing of personal data by an internet search engine*

70. The first sub-question in this group concerns the applicability of the notions of 'personal data' and 'processing' thereof to a internet search engine service provider such as Google, on the assumption that we are not discussing personal data of users or advertisers, but personal data

published on third-party source web pages, and processed by internet search engine operated by the service provider. This processing is described by the national court as consisting of locating information published or included on the internet by third parties, indexing it automatically, storing it temporarily and finally, making it available to internet users according to a particular order of preference.

71. In my opinion an affirmative answer to this sub-question does not require much discussion. The concept of personal data is given a wide definition in the Directive, this wide definition has been applied by the Article 29 Working Party and it has been confirmed by the Court. (48)

72. As to 'processing', source web pages on the internet may and often do include names, images, addresses, telephone numbers, descriptions and other indications, with the help of which a natural person can be identified. The fact that their character as personal data would remain 'unknown' to internet search engine service provider, whose search engine works without any human interaction with the data gathered, indexed and displayed for search purposes, does not change this finding. (49) The same applies to the fact that the presence of personal data in the source web pages is in a certain sense random for the internet search engine service provider because for the service provider, or more precisely for the crawling, analysing and indexing functions of the search engine targeting all web pages accessible on the internet, there may be no technical or operational difference between a source web page containing personal data and another not including such data. (50) In my opinion these facts should, however, influence the interpretation of the concept of 'controller'.

73. Google's search engine's crawler function, called 'googlebot', crawls on the internet constantly and systematically and, advancing from one source web page to another on the basis of hyperlinks between the pages, requests the visited sites to send to it a copy of the visited page. (51) The copies of such source web pages are analysed by Google's indexing function. Sign strings (keywords, search terms) found on the pages are recorded in the index of the search engine. (52) Google's elaborate search algorithm also assesses the relevance of the search results. The combinations of these keywords with the URL addresses, where they can be found, form the index of the search engine. The searches initiated by the users are executed within the index. For the purposes of indexing and displaying the search results, the copy of the pages is registered in the cache memory of the search engine. (53)

74. A copy of the sought source web page, stored in cache, can be displayed after the user has made the search. However, the user can access the original page if, for example, he seeks the display of pictures in the source web page. The cache is updated frequently but there may be situations where the page displayed by the search engine does not correspond to the source web pages in the host server because of the changes made to it or its deletion. (54)

75. It goes without saying that the operations described in the previous paragraphs count as 'processing' of the personal data on the source web pages copied, indexed, cached and displayed by the search engine. More particularly they entail collection, recording, organisation and storage of such personal data and they may entail their use, disclosure by transmission, dissemination or otherwise making available and combining of personal data in the sense of Article 2(b) of the Directive.

B – *The concept of 'controller'*

76. A controller (55) is according to Article 2(d) of the Directive 'the natural or legal person … which alone or jointly with others determines the purposes and means of the processing of personal data'. In my opinion the core issue in this case is whether, and to what extent, an internet search

engine service provider is covered by this definition.

77. All parties except for Google and the Greek Government propose an affirmative answer to this question, which might easily be defended as a logical conclusion of a literal and perhaps even teleological interpretation of the Directive, given that the basic definitions of the Directive were formulated in a comprehensive manner in order to cover new developments. In my opinion such an approach would, however, represent a method that completely ignores the fact that when the Directive was drated it was not possible to take into account the emergence of the internet and the various related new phenomena.

78. When the Directive was adopted the World Wide Web had barely become a reality, and search engines were at their nascent stage. The provisions of the Directive simply do not take into account the fact that enormous masses of decentrally hosted electronic documents and files are accessible from anywhere on the globe and that their contents can be copied and analysed and disseminated by parties having no relation whatsoever to their authors or those who have uploaded them onto a host server connected to the internet.

79. I recall that in *Lindqvist* the Court did not follow the maximalist approach proposed by the Commission in relation to the interpretation of the notion of transfer of data to third countries. The Court stated that '[given], first, the state of development of the internet at the time [the Directive] was drawn up and, second, the absence, in Chapter IV, of criteria applicable to the use of internet, one cannot presume that the Community legislature intended the expression "transfer [of data] to a third country" to cover the loading, by an individual in Mrs Lindqvist's position, of data onto an internet page, even if those data are thereby made accessible to persons in third countries with the technical means to access them'. (56) In my opinion this implies that in the interpretation of the Directive, vis-à-vis new technological phenomena, the principle of proportionality, the objectives of the Directive and means provided therein for their attainment must be taken into account in order to achieve a balanced and reasonable outcome.

80. To my mind, one key question here is whether it matters that within the definition of controller the Directive refers to the controller as the person 'determining the purposes and means of the processing of the *personal* data' (emphasis added). The parties who consider Google to be a controller base this assessment on the undeniable fact that the service provider running an internet search engine determines the purposes and means of the processing of *data* for his purposes.

81. I doubt, however, whether this leads to a truthful construction of the Directive in a situation where the object of processing consists of files containing personal data and other data in a haphazard, indiscriminate and random manner. Does the European law professor mentioned in my example in paragraph 29 above determine the purposes and means of the processing of *personal data* included in the Court's judgments he has downloaded to his laptop? The finding of the Article 29 Working Party according to which 'users of the search engine service could strictly speaking also be considered as controllers' reveals the irrational nature of the blind literal interpretation of the Directive in the context of the internet. (57) The Court should not accept an interpretation which makes a controller of processing of personal data published on the internet of virtually everybody owning a smartphone or a tablet or a laptop computer.

82. In my opinion the general scheme of the Directive, most language versions and the individual obligations it imposes on the controller are based on the idea *of responsibility of the controller* over the *personal* data processed in the sense that the *controller* is aware of the existence of a certain defined category of information amounting to personal data and the controller processes this data with some intention which relates to their processing *as* personal data. (58)

83. The Article 29 Working Party correctly notes that '[t]he concept of controller is a functional concept, intended to allocate responsibilities where the factual influence is, and thus based on a factual rather than a formal analysis'. (59) It continues that 'the controller must determine which data shall be processed for the purpose(s) envisaged'. (60) The substantive provisions of the Directive, and more particularly Articles 6, 7 and 8 thereof, are, in my opinion, based on the assumption that the controller knows what he is doing in relation to the personal data concerned, in the sense that he is aware of what kind of personal data he is processing and why. In other words, the data processing must appear to him as processing of personal data, that is 'information relating to an identified or identifiable natural person' in some semantically relevant way and not a mere computer code. (61)

C – *An internet search engine service provider is not a 'controller' of personal data on third-party source web pages*

84. The internet search engine service provider merely supplying an information location tool does not exercise control over personal data included on third-party web pages. The service provider is not 'aware' of the existence of personal data in any other sense than as a statistical fact web pages are likely to include personal data. In the course of processing of the source web pages for the purposes of crawling, analysing and indexing, personal data does not manifest itself as such in any particular way.

85. It is for this reason that I find the approach of the Article 29 Working Party adequate as it seeks to draw a line between the entirely passive and intermediary functions of search engines and situations where their activity represents real control over the personal data processed. (62) For the sake of completeness, it needs to be added that issue of whether the personal data has become public (63) or has been disclosed legally on third-party source web pages is not relevant for application of the Directive. (64)

86. The internet search engine service provider has no relationship with the content of third-party source web pages on the internet where personal data may appear. Moreover, as the search engine works on the basis of copies of the source web pages that its crawler function has retrieved and copied, the service provider does not have any means of changing the information in the host servers. Provision of an information location tool does not imply any control over the content. It does not even enable the internet search engine service provider to distinguish between personal data, in the sense of the Directive, that relates to an identifiable living natural person, and other data.

87. Here I would draw from the principle expressed in recital 47 in the preamble to the Directive. It states that the controller of messages containing personal data transmitted by telecommunication or by electronic mail is the *originator* of the message and not the person offering transmission services. This recital, as well as the exceptions to liability provided in the ecommerce Directive 2000/31 (Articles 12, 13 and 14), builds on the legal principle according to which automated, technical and passive relationships to electronically stored or transmitted content do not create control or liability over it.

88. The Article 29 Working Party has emphasised that, first and foremost, the purpose of the concept of controller is to determine who is to be responsible for compliance with data protection rules and to allocate this responsibility to the *locus* of the factual influence. (65) According to the Working Party, '[t]he principle of proportionality requires that to the extent that a search engine provider acts purely as an intermediary, it should not be considered as the principal controller with regard to the content related processing of personal data that is taking place. In this case the principal controllers of personal data are the information providers.' (66)

89. In my view the internet search engine service provider cannot in law or in fact fulfil the obligations of controller provided in Articles 6, 7 and 8 of the Directive in relation to the personal data on source web pages hosted on third-party servers. Therefore a reasonable interpretation of the Directive requires that the service provider is not generally considered as having that position. (67)

90. An opposite opinion would entail internet search engines being incompatible with EU law, a conclusion I would find absurd. Specifically, if internet search engine service providers were considered as controllers of the personal data on third-party source web pages and if on any of these pages there would be 'special categories of data' referred to in Article 8 of the Directive (e.g. personal data revealing political opinions or religious beliefs or data concerning the health or sex life of individuals), the activity of the internet search engine service provider would automatically become illegal, when the stringent conditions laid down in that article for the processing of such data were not met.

D – *Circumstances in which the internet search engine service provider is a 'controller'*

91. Internet search engine service provider clearly controls the index of the search engine which links key words to the relevant URL addresses. The service provider determines how the index is structured, and it may technically block certain search results, for example by not displaying URL addresses from certain countries or domains within the search results. (68) Moreover, the internet search engine service provider controls its index in the sense that he decides whether exclusion codes (69) on source web page are to be complied with or not.

92. In contrast, the contents of the cache memory of the internet search engine cannot be considered as falling within the control of the service provider because the cache is the result of completely technical and automated processes producing a mirror image of the text data of the crawled web pages, with the exception of data excluded from indexing and archiving. It is of interest that some Member States seem to provide special horizontal exceptions regarding the liability of search engines analogous to the exception provided in ecommerce Directive 2000/31 for certain information society service providers. (70)

93. However, with regard to the contents of cache, a decision not to comply with the exclusion codes (71) on a web page entails in my opinion control in the sense of the Directive over such personal data. The same applies in situations where the internet search engine service provider does not update a web page in its cache despite a request received from the website.

E – *The obligations of an internet search engine service provider as 'controller'*

94. It is obvious that if and when the internet search engine service provider can be considered as 'controller' he must comply with the obligations provided by the Directive.

95. As to the criteria relating making data processing legitimate in the absence of a data subject's consent (Article 7(a) of the Directive), it seems obvious that provision of internet search engine services pursues as such legitimate interests (Article 7(f) of the Directive), namely (i) making information more easily accessible for internet users; (ii) rendering dissemination of the information uploaded on the internet more effective; and (iii) enabling various information society services supplied by the internet search engine service provider that are ancillary to the search engine, such as the provision of keyword advertising. These three purposes relate respectively to three fundamentals rights protected by the Charter, namely freedom of information and freedom of expression (both in Article 11) and freedom to conduct a business (Article 16). Hence, an internet search engine service provider pursues legitimate interests, within the meaning of Article 7(f) of the Directive, when he processes data made available on the internet, including personal data.

96. As controller, an internet search engine service provider must respect the requirements laid down in Article 6 of the Directive. In particular, the personal data must be adequate, relevant, and not excessive in relation to the purposes for which they are collected, and up to date, but not out dated for the purposes for which they were collected. Moreover, the interests of the 'controller', or third parties in whose interest the processing in exercised, and those of the data subject, must be weighed.

97. In the main proceedings, the data subject's claim seeks to remove from Google's index the indexing of his name and surnames with the URL addresses of the newspaper pages displaying the personal data he is seeking to suppress. Indeed, names of persons are used as search terms, and they are recorded as keywords in search engines' indexes. Yet, usually a name does not as such suffice for *direct* identification of a natural person on the internet because globally there are several, even thousands or millions of persons with the same name or combination of a given name(s) and surname. (72) Nevertheless, I assume that in most cases combining a given name and surname as a search term enables the *indirect* identification of a natural person in the sense of Article 2(a) of the Directive as the search result in a search engine's index reveals a limited set of links permitting the internet user to distinguish between persons with the same name.

98. A search engine's index attaches names and other identifiers used as a search term to one or several links to web pages. Inasmuch as the link is adequate in the sense that the data corresponding to the search term really appears or has appeared on the linked web pages, the index in my opinion complies with the criteria of adequacy, relevancy, proportionality, accuracy and completeness, set out in Articles 6(c) and 6(d) of the Directive. As to the temporal aspects referred to in Articles 6(d) and 6(e) (personal data being up to date and personal data not being stored longer than necessary), these issues should also be addressed from the point of view of the processing in question, that is provision of information location service, and not as an issue relating to the content of the source web pages. (73)

F – *Conclusion on the second group of questions*

99. On the basis of this reasoning, I take the view that a national data protection authority cannot require an internet search engine service provider to withdraw information from its index except for the cases where this service provider has not complied with the exclusion codes (74) or where a request emanating from the website regarding update of cache memory has not been complied with. This scenario does not seem pertinent for the present preliminary reference. A possible 'notice and take down procedure' (75) concerning links to source web pages with illegal or inappropriate contents is a matter of national law civil liability based on grounds other than the protection of personal data. (76)

100. For these reasons I propose that the Court answers the second group of questions in the sense that under the circumstances specified in the preliminary reference an internet search engine service provider 'processes' personal data in the sense of Article 2(b) of the Directive. However, the service provider cannot be considered as 'controller' of the processing of such personal data in the sense of Article 2(d) of the Directive with the exception explained above.

VII – Third question relating to the data subject's possible 'right to be forgotten'

A – *Preliminary observations*

101. The third preliminary question is only relevant if the Court either rejects the conclusion I have reached above to the effect that Google is not generally to be considered as a 'controller' under Article 2(d) of the Directive, or to the extent the Court accepts my assertion that there are instances

where an internet search engine service provider such as Google could be considered as having such a position. Otherwise, the section that follows is redundant.

102. In any event, by its third question the national court asks whether the rights to erasure and blocking of data, provided for in Article 12(b) of the Directive, and the right to object, provided for in Article 14(a) of the Directive, extend to enabling the data subject to contact the internet search engine service providers himself in order to prevent indexing of the information relating to him personally that has been published on third parties' web pages. By so doing, a data subject seeks to prevent potentially prejudicial information from being known to internet users, or is expressing a desire for the information to be consigned to oblivion, even though the information in question has been lawfully published by third parties. In other words the national court asks in substance whether a 'right to be forgotten' can be founded on Article 12(b) and 14(a) of the Directive. This is the first issue to be addressed in the analysis that follows, which will be based on the wording and objectives of those provisions.

103. If I conclude that Articles 12(b) and 14(a) of the Directive, in and of themselves, do not afford this protection, I will then consider whether such an interpretation is compatible with the Charter. (77) This will require consideration of the right to protection of personal data in Article 8, right to respect for private and family life in Article 7, freedom of expression and information as protected in Article 11 (and both with respect to the freedom of expression of publishers of web pages and the freedom of internet users to receive information), and the freedom to conduct a business in Article 16. Indeed, the rights of data subjects in Articles 7 and 8 will need to be juxtaposed against the rights protected by Articles 11 and 16 of those who wish to disseminate or access the data.

B – *Do the rights to rectification, erasure, blocking and objection provided in the Directive amount to a data subject's right 'to be forgotten'?*

104. The rights to rectification, erasure and blocking of data provided in Article 12(b) of the Directive concern data, the processing of which does not comply with the provisions of the Directive, *in particular* because of the incomplete or inaccurate nature of the data (my emphasis).

105. The order for reference recognises that the information appearing on the web pages concerned cannot be regarded as incomplete or inaccurate. Even less is it claimed that Google's index or the contents of its cache containing such data may be so described. Therefore, the right to rectification, erasure or blocking, referred to in Article 12(b) of the Directive, will only arise if Google's processing of personal data from third-party source web pages is incompatible with the Directive for other reasons.

106. Article 14(a) of the Directive obliges Member States to grant a data subject the right to object at any time, on compelling legitimate grounds relating to his particular situation, to the processing of data relating to him, save where otherwise provided by national legislation. This applies especially in cases referred to in Articles 7(e) and 7(f) of the Directive, that is where processing is necessary in view of a public interest or for the purposes of the legitimate interests pursued by the controller or by third parties. Furthermore, according to Article 14(a), 'the processing instigated by the controller' may no longer involve the objected data if the objection is justified.

107. In the situations where internet search engine service providers are considered to be controllers of the processing of personal data, Article 6(2) of the Directive obliges them to weigh the interests of the data controller, or third parties in whose interest the processing is exercised, against those of the data subject. As the Court observed in *ASNEF and FECEMD*, whether or not the data in question already appears in public sources is relevant to this balancing exercise. (78)

108. However, as almost all of the parties having presented written observations in this case have asserted, I consider that the Directive does not provide for a general right to be forgotten in the sense that a data subject is entitled to restrict or terminate dissemination of personal data that he considers to be harmful or contrary to his interests. The purpose of processing and the interests served by it, when compared to those of the data subject, are the criteria to be applied when data is processed without the subject's consent, and not the subjective preferences of the latter. A subjective preference alone does not amount to a compelling legitimate ground within the meaning of Article 14(a) of the Directive.

109. Even if the Court were to find that internet search engine service providers were responsible as controllers, *quod non*, for personal data on third-party source web pages, a data subject would still not have an absolute 'right to be forgotten' which could be relied on against these service providers. However, the service provider would need to put itself in the position of the publisher of the source web page and verify whether dissemination of the personal data on the page can at present be considered as legal and legitimate for the purposes of the Directive. In other words, the service provider would need to abandon its intermediary function between the user and the publisher and assume responsibility for the content of the source web page, and when needed, to censure the content by preventing or limiting access to it.

110. For the sake of completeness it is useful to recall that the Commission Proposal for a General Data Protection Regulation provides in its Article 17 for a right to be forgotten. However, the proposal seems have met with considerable opposition, and it does not purport to represent a codification of existing law, but an important legal innovation. Therefore it does not seem affect the answer to be given to the preliminary question. It is of interest, however, that according to Article 17(2) of the proposal '[w]here the controller … has made the personal data public, it shall take all reasonable steps … in relation to data for the publication of which the controller is responsible, to inform third parties which are processing such data, that a data subject requests them to erase any links to, or copy or replication of that personal data'. This text seems to consider internet search engine service providers more as third parties than as controllers in their own right.

111. I therefore conclude that Articles 12(b) and 14(a) of the Directive do not provide for a right to be forgotten. I will now consider whether this interpretation of these provisions complies with the Charter.

C – *The fundamental rights in issue*

112. Article 8 of the Charter guarantees everyone the right to the protection of his personal data. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned, or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him, and the right to have it rectified. Compliance with these rules shall be subject to control by an independent authority.

113. In my opinion this fundamental right, being a restatement of the European Union and Council of Europe *acquis* in this field, emphasises the importance of protection of personal data, but it does not as such add any significant new elements to the interpretation of the Directive.

114. According to Article 7 of the Charter, everyone has the right to respect for his or her private and family life, home and communications. This provision, being in substance identical to Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms, signed in Rome on 4 November 1950 (ECHR), must be duly taken into account in the interpretation of the relevant provisions of the Directive, which requires the Member States to protect *in particular* the right to privacy.

115. I would recall that in the context of the ECHR, Article 8 thereof also covers issues relating to protection of personal data. For this reason, and in conformity with Article 52(3) of the Charter, the case-law of the European Court of Human Rights on Article 8 ECHR is relevant both to the interpretation of Article 7 of the Charter and to the application of the Directive in conformity with Article 8 of the Charter.

116. The European Court of Human Rights concluded in *Niemietz* that professional and business activities of an individual may fall within the scope of private life as protected under Article 8 ECHR. (79) This approach has been applied in subsequent case-law of that court.

117. Moreover, this Court found in *Volker und Markus Schecke and Eifert* (80) that 'the right to respect for private life with regard to the processing of personal data, recognised by Articles 7 and 8 of the Charter, concerns *any information* [my emphasis] relating to an identified or identifiable individual … and the limitations which may lawfully be imposed on the right to protection of personal data correspond to those tolerated in relation to Article 8 [ECHR]'.

118. I conclude on the basis of *Volker und Markus Schecke and Eifert* that the protection of private life under the Charter, with regard to the processing of personal data, covers all information relating to an individual irrespective of whether he acts in a purely private sphere or as an economic operator or, for example, as a politician. In view of the the wide notions of personal data and its processing in EU law, it seems to follow from abovementioned case-law that any act of communication relying on automatic means such as by means of telecommunications, e-mail or social media concerning a natural person constitutes as such a putative interference of that fundamental right that requires justification. (81)

119. I have concluded in paragraph 75 that an internet search engine service provider is engaged in processing of personal data displayed on third-party source web pages. Hence it follows from the Court's judgment in *Volker und Markus Schecke and Eifert* that, independently of how his role is classified under the Directive, there is interference with the Article 7 Charter right to privacy of the concerned data subjects. According to the ECHR and the Charter any interference to protected rights must be based on law and be necessary in a democratic society. In the present case we are not faced with interference by public authorities in need of justification but of the question of the extent that interference by private subjects can be tolerated. The limits to this are set out in the Directive, and they are thus based on law, as required by the ECHR and the Charter. Hence, when the Directive is interpreted, the exercise precisely concerns the interpretation of the limits set to data processing by private subjects in light of the Charter. From this follows the question of whether there is a positive obligation on the EU and the Member States to enforce, as against internet search engine service providers, which are private subjects, a right to be forgotten. (82) This in turn leads to questions of justification for interference in Article 7 and 8 of the Charter, and the relationship with the competing rights of freedom of expression and information, and the right to conduct a business.

D – *Rights of freedom of expression and information, and the right to conduct a business*

120. The present case concerns, from many angles, freedom of expression and information enshrined in Article 11 of the Charter, which corresponds to Article 10 ECHR. Article 11(1) of the Charter states that '[e]veryone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers.' (83)

121. The internet users' right to seek and receive information made available on the internet is protected by Article 11 of the Charter. (84) This concerns both information on the source web pages

and the information provided by internet search engines. As I have already mentioned, the internet has revolutionalised access to and dissemination of all kinds of information and enabled new forms of communication and social interaction between individuals. In my opinion the fundamental right to information merits particular protection in EU law, especially in view of the ever-growing tendency of authoritarian regimes elsewhere to limit access to the internet or to censure content made accessible by it. (85)

122. Publishers of web pages equally enjoy protection under Article 11 of the Charter. Making content available on the internet counts as such as use of freedom of expression, (86) even more so when the publisher has linked his page to other pages and has not limited its indexing or archiving by search engines, thereby indicating his wish for wide dissemination of content. Web publication is a means for individuals to participate in debate or disseminate their own content or content uploaded by others on internet. (87)

123. In particular, the present preliminary reference concerns personal data published in the historical archives of a newspaper. In *Times Newspapers Ltd v. the United Kingdom (nos. 1 and 2)*, the European Court of Human Rights observed that internet archives make a substantial contribution to preserving and making available news and information: 'Such archives constitute an important source for education and historical research, particularly as they are readily accessible to the public and are generally free. … However, the margin of appreciation afforded to States in striking the balance between the competing rights is likely to be greater where news archives of past events, rather than news reporting of current affairs, are concerned. In particular, the duty of the press to act in accordance with the principles of responsible journalism by ensuring *accuracy* [my emphasis] of historical, rather than perishable, information published is likely to be more stringent in the absence of any urgency in publishing the material.' (88)

124. Commercial internet search engine service providers offer their information location services in the context of business activity aiming at revenue from keyword advertising. This makes it a business, the freedom of which is recognised under Article 16 of the Charter in accordance with EU law and national law. (89)

125. Moreover, it needs to be recalled that none of the fundamental rights at stake in this case are absolute. They may be limited provided that there is a justification acceptable in view of the conditions set out in Article 52(1) of the Charter. (90)

E – *Can a data subject's 'right to be forgotten' be derived from Article 7 of the Charter?*

126. Finally, it is necessary to ponder whether interpretation of Articles 12(b) and 14(a) of the Directive in light of the Charter, and more particularly of Article 7 thereof, could lead to the recognition of a 'right to be forgotten' in the sense referred to by the national court. At the outset such a finding would not be against Article 51(2) of the Charter because it would concern precision of the scope of the data subject's right of access and right to object already recognised by the Directive, not the creation of new rights or widening the scope of EU law.

127. The European Court of Human Rights held in the *Aleksey Ovchinnikov* case (91) that 'in certain circumstances a restriction on reproducing information that has already entered the public domain may be justified, for example to prevent further airing of the details of an individual's private life which do not come within the scope of any political or public debate on a matter of general importance'. The fundamental right to protection of private life can thus in principle be invoked even if the information concerned is already in the public domain.

128. However, a data subject's right to protection of his private life must be balanced with other

fundamental rights, especially with freedom of expression and freedom of information.

129. A newspaper publisher's freedom of information protects its right to digitally republish its printed newspapers on the internet. In my opinion the authorities, including data protection authorities, cannot censure such republishing. The *Times Newspapers Ltd v. the United Kingdom (nos. 1 and 2)* judgment of the European Court of Human Rights (92) demonstrates that the liability of the publisher regarding *accuracy* of historical publications may be more stringent than those of current news, and may require the use of appropriate *caveats supplementing* the contested content. However, in my opinion there could be no justification for requiring digital republishing of an issue of a newspaper with content different from the originally published printed version. That would amount to falsification of history.

130. The data protection problem at the heart of the present litigation only appears if an internet user types the data subject's name and surnames into the search engine, thereby being given a link to the newspaper's web pages with the contested announcements. In such a situation the internet user is *actively using his right to receive information concerning the data subject from public sources* for reasons known only to him. (93)

131. In contemporary information society, the right to search information published on the internet by means of search engines is one of the most important ways to exercise that fundamental right. This right undoubtedly covers the right to seek information relating to other individuals that is, in principle, protected by the right to private life such as information on the internet relating to an indivdual's activities as a businessman or politician. An internet user's right to information would be compromised if his search for information concerning an individual did not generate search results providing a truthful reflection of the relevant web pages but a 'bowdlerised' (94) version thereof.

132. An internet search engine service provider lawfully exercises both his freedom to conduct business and freedom of expression when he makes available internet information location tools relying on a search engine.

133. The particularly complex and difficult constellation of fundamental rights that this case presents prevents justification for reinforcing the data subjects' legal position under the Directive, and imbuing it with a right to be forgotten. This would entail sacrificing pivotal rights such as freedom of expression and information. I would also discourage the Court from concluding that these conflicting interests could satisfactorily be balanced in individual cases on a case-by-case basis, with the judgment to be left to the internet search engine service provider. Such 'notice and take down procedures', if required by the Court, are likely either to lead to the automatic withdrawal of links to any objected contents or to an unmanageable number of requests handled by the most popular and important internet search engine service providers. (95) In this context it is necessary to recall that 'notice and take down procedures' that appear in the ecommerce Directive 2000/31 relate to unlawful content, but in the context of the case at hand we are faced with a request for suppressing legitimate and legal information that has entered the public sphere.

134. In particular, internet search engine service providers should not be saddled with such an obligation. This would entail an interference with the freedom of expression of the publisher of the web page, who would not enjoy adequate legal protection in such a situation, any unregulated 'notice and take down procedure' being a private matter between the data subject and the search engine service provider. (96) It would amount to the censuring of his published content by a private party. (97) It is a completely different thing that the States have positive obligations to provide an effective remedy against the publisher infringing the right to private life, which in the context of internet would concern the publisher of the web page.

135. As the Article 29 Working Party has observed, it is possible that the secondary liability of the search engine service providers under national law may lead to duties amounting to blocking access to third-party websites with illegal contents such as web pages infringing IP rights, or displaying libellous or criminal information. (98)

136. In contrast any generalised right to be forgotten cannot be invoked against them on the basis of the Directive even when it is interpreted in harmony with the Charter.

137. For these reasons I propose that the Court should answer the third preliminary question to the effect that the rights to erasure and blocking of data, provided for in Article 12(b), and the right to object, provided for by Article 14(a), of the Directive, do not extend to such a right to be forgotten as described in the preliminary reference.

VIII – Conclusion

138. In the light of the above considerations, I am of the opinion that the Court should reply as follows to the questions referred by the Audiencia Nacional:

1. Processing of personal data is carried out in the context of the activities of an 'establishment' of the controller within the meaning of Article 4(1)(a) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data when the undertaking providing the internet search engine sets up in a Member State, for the purposes of promoting and selling advertising space on the search engine, an office or subsidiary which orientates its activity towards the inhabitants of that State.

2. An internet search engine service provider, whose search engine locates information published or included on the internet by third parties, indexes it automatically, stores it temporarily and finally makes it available to internet users according to a particular order of preference, 'processes' personal data in the sense of Article 2(b) of Directive 95/46 when that information contains personal data.

However, the internet search engine service provider cannot be considered as 'controller' of the processing of such personal data in the sense of Article 2(d) of Directive 95/46, with the exception of the contents of the index of its search engine, provided that the service provider does not index or archive personal data against the instructions or requests of the publisher of the web page.

3. The rights to erasure and blocking of data, provided for in Article 12(b), and the right to object, provided for in Article 14(a), of Directive 95/46, do not confer on the data subject a right to address himself to a search engine service provider in order to prevent indexing of the information relating to him personally, published legally on third parties' web pages, invoking his wish that such information should not be known to internet users when he considers that it might be prejudicial to him or he wishes it to be consigned to oblivion.

---

1 – Original language: English.

---

2 – *Harvard Law Review*, Vol. IV, No 5, 15 December 1890,.

---

3 – In actual fact the 'internet' comprises two main services, namely the World Wide Web and email services. While the internet, as a network of interconnected computers, has existed in various forms for some time, commencing with the Arpanet (United States), the freely accessible open network with www

addresses and common code structure only started in the early 1990s. It seems that the historically correct term would be World Wide Web. However, given the current usage and terminological choices made in Court's case-law, in the following the word 'internet' is primarily used to refer to the World Wide Web part of the network.

---

4 – The location of web pages is identified with an individual address, the 'URL' (Uniform Resource Locator), a system created in 1994. A web page can be accessed by typing its URL in the web browser, directly or with the help of a domain name. The web pages must be coded with some markup language. HyperText Markup Language (HTML) is the main markup language for creating web pages and other information that can be displayed in a web browser.

---

5 – The scope of the three issues is illustrated by the following information (although no exact figures are available). First, it has been estimated that there could be more than 600 million websites on the internet. On these websites there appears to be more than 40 billion web pages. Second, with regard to the search engines, their number is much more limited: it appears that there are less than 100 important search engines, and currently Google seems to have a huge share in many markets. It has been said that success of Google's search engine is based on very powerful web crawlers, efficient indexing systems and technology that allows the search results to be sorted by their relevance to the user (including the patended PageRank algorithm), see López-Tarruella, A., 'Introduction: Google Pushing the Boundaries of Law', *Google and the Law. Empirical Approaches to Legal Aspects of Knowledge-Economy Business Models*, Ed. López-Tarruella, A., T.M.C. Asser Press, The Hague, 2012, pp. 1-8, p. 2. Third, more than three quarters of people in Europe use the internet and in so far that they use the search engines, their personal data, as internet search engine users, may be gathered and processed by the internet search engine used.

---

6 – Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31).

---

7 – See, in general, Article 29 Working Party, Opinion 1/2008 on data protection issues related to search engines (WP 148). Google's privacy policy, as regards the users of its internet search engine, is under scrutiny by the data protection authorities of the Member States. The action is lead by the French Data Protection Authority (the CNIL). For recent developments, see letter dated 16 October 2012 of Article 29 Working Party to Google, available on website mentioned in footnote 22 below.

---

8 – Point 19 below.

---

9 – In the following, 'internet search engine' refers to the combination of software and equipment enabling the feature of searching text and audiovisual content on the internet. Specific issues relating to search engines operating within a defined internet domain (or website) such as http://curia.europa.eu are not discussed in this opinion. The economic operator providing for access to a search engine is referred to as the 'internet search engine service provider'. In the present case Google Inc. appears to be the service provider providing access to Google search engine as well as many additional search functions such as maps.google.com and news.google.com.

---

10 – Case C-101/01 *Lindqvist* [2003] ECR I-12971.

---

11 – Joined Cases C-465/00, C-138/01 and C-139/01 *Österreichischer Rundfunk and Others* [2003] ECR I-4989.

---

12 – Case C-73/07 *Satakunnan Markkinapörssi and Satamedia* [2008] ECR I-9831.

---

13 – Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke and Eifert* [2010] ECR I-0000.

---

14 – Joined Cases C-236/08 to C-238/08 *Google France and Google* [2010] ECR I-2417; Case C-558/08 *Portakabin* [2010] ECR I-6963; Case C-324/09 *L'Oréal and Others* [2011] ECR I-0000; Case C-323/09 *Interflora and Interflora British Unit* [2011] ECR I-0000; and Case C-523/10 *Wintersteiger* [2012] ECR I-0000.

---

15 – Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regards to the processing of personal data and on the free movement of such data (General Data Protection Regulation). COM(2012)11 final.

---

16 – BOE No 298, 14 December 1999, p. 43088.

---

17 – According to its recital 11, the 'principles of the protection of the rights and freedoms of individuals, notably the right to privacy, which are contained in this Directive, give substance to and amplify those contained in the Council of Europe Convention of 28 January 1981 for the protection of individuals with regard to automatic processing of personal data'.

18– Article 29 Working Party, Opinion 1/2010 on the concepts of 'controller' and 'processor' (WP 169), pp. 3-4.

---

19 – For example, Joined Cases C-509/09 and C-161/10 *eDate Advertising and Martinez* [2011] ECR I-0000, paragraph 45.

---

20 – A newspaper normally includes personal data such as names of natural persons. This personal data is processed when it is consulted by automatic means. This processing is within the scope of application of the Directive unless it is exercised by a natural person in the course of a purely personal or household activity. See Article 2(a) and (b) and Article 3(2) of the Directive. Moreover, reading a paper document or displaying images including personal data also amounts to its processing. See Dammann, U. and Simitis, S., *EG-Datenschutzrichtlinie*, Nomos Verlagsgesellschaft, Baden-Baden, 1997, p. 110.

---

21 – *Lindqvist*, points 67–70, as regards the interpretation of Article 25 of the Directive.

---

22 – The opinions are available at http://ec.europa.eu/justice/data-protection/index_en.htm.

---

23 – Internet search engines develop constantly and the purpose here is only to give an overview of the salient features that are currently relevant.

---

24 – Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) (OJ 2000 L 178, p. 1).

---

25 – See recital 18 in the preamble to and Article 2(a) of ecommerce Directive 2000/31, read together with Article 1(2) of Directive 98/34/EC of the European Parliament and of the Council of 22 June 1998 laying down a procedure for the provision of information in the field of technical standards and regulations and of rules on information society services (OJ 1998 L 204, p. 37), as amended by Directive 98/48/EC of the European Parliament and of the Council of 20 July 1998 (OJ 1998 L 217, p. 18).

---

26 – *Lindqvist*, paragraphs 25-27.

---

27 – A typical current exclusion code (or robot exclusion protocol) is called ‘robots.txt’; see http://en.wikipedia.org/wiki/Robots.txt or http://www.robotstxt.org/.

---

28 – Exclusion codes do not, however, technically prevent indexing or displaing, but the service provider running a search engine can decide to ignore them. Major internet search engine service providers, Google included, claim that they comply with such codes included in the source web page. See the Article 29 Working Party, Opinion 1/2008, p. 14.

---

29 – See the judgment of the European Court of Human Rights, *K.U. v. Finland*, no. 2872/02, § 43 and § 48, ECHR 2008, where the Court referred to the existence of positive obligations inherent in an effective respect for private or family life. These obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of the relations of individuals between themselves. In *K.U. v. Finland* the State had a positive obligation to ensure that an effective remedy was available against the publisher.

---

30 – However, the internet is not a single enormous data bank established by the ‘Big Brother’ but a decentralised system of information originating from innumerable independent sources where accessibility and dissemination of information rely on intermediary services having as such nothing to do with the contents.

---

31 – See, in this respect, my opinion in *L’Oréal and Others*, points 54 et seq.

---

32 – This corresponds to the third situation mentioned in paragraph 3 above.

---

33 – For an example of a keywords advertising system (Google’s AdWords) see *Google France and*

Google, paragraphs 22 and 23; Case C-278/08 *BergSpechte* [2010] ECR I-2517, paragraphs 5-7; *Portakabin*, paragraphs 8-10; and *Interflora and Interflora British Unit*, paragraphs 9-13.

---

34 – Case C-400/10 PPU *McB.* [2010] ECR I-8965, paragraphs 51 and 59; Case C-256/11 *Dereci and Others* [2011] ECR I-0000, paragraphs 71 and 72; Case C-40/11 *Iida* [2012] ECR I-0000, paragraph 78; and Case C-617/10 *Åkerberg Fransson* [2013] ECR I-0000, paragraph 23.

---

35 – For example in *McB.* the Court resisted an interpretation, which was sought on the basis of Article 7 of the Charter, of 'rights of custody' in Article 2(9) of Council Regulation (EC) No 2201/2003 of 27 November 2003 concerning jurisdiction and the recognition and enforcement of judgments in matrimonial matters and the matters of parental responsibility, repealing Regulation (EC) No 1347/2000 (OJ 2003 L 338, p. 1) that would have enlarged its meaning. That said, of course, if it is impossible to interpret an EU legislative provision in conformity with fundamental rights protected by EU law, that provision must be declared invalid. See Case C-236/09 *Association belge des Consommateurs Test-Achats and Others* [2011] ECR I-773, paragraphs 30-34.

---

36 – Article 29 Working Party, Opinion 8/2010 on applicable law (WP 179), p. 8.

---

37 – Article 29 Working Party, Opinion 8/2010, pp. 24 and 31.

---

38 – Article 3(2)(a) of the Commission Proposal.

---

39 – *L'Oréal and Others* and the ecommerce Directive 2000/31.

---

40 – Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (OJ 2001 L 12, p. 1), Joined Cases C-585/08 and C-144/09 *Pammer and Hotel Alpenhof* [2010] ECR I-12527, and *Wintersteiger*. See also my Opinion in Case C-170/12 *Pinckney*, pending.

---

41 – Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (OJ 2001 L 167, p. 10) and Case C-5/11 *Donner* [2012] ECR I-0000.

---

42 – The reference does not specify what is meant by 'centre of gravity', but this expression was used by Advocate General Cruz Villalón in his Opinion in *eDate Advertising and Martinez*, points 32 and 55.

---

43 – Article 29 Working Party, Opinion 8/2010, pp. 8 and 9. The Working Party also points out that the word 'equipment' used in the English version of the Directive is too narrow because the other language versions speak about 'means' which also covers non-material devices such as cookies (pp. 20 and 21).

---

44 – See, in particular, Article 29 Working Party, Opinion 8/2010, p. 19 where it is submitted that Article 4(1)(c) of the Directive should apply, despite its wording, where the controller has establishments

in the EU but their activities are unrelated to the concerned processing of personal data.

---

45 – See *Google France and Google*, paragraph 23.

---

46 – See *Google France and Google*, paragraph 25, and Article 29 Working Party, Opinion 1/2008, pp. 5-6. It is easy to verify that the use of the same keywords on different national Google domains may trigger the display of different search results and advertisements.

---

47 – Article 29 Working Party, Opinion 1/2008, p. 10.

---

48 – See Article 2(a) of the Directive, according to which personal data means 'any information relating to an identified or identifiable natural person'. A wide range of examples is given by Article 29 Working Party, in its Opinion 4/2007 on the concept of personal data (WP 136). The Court confirmed the wide interpretation in *Lindqvist*, paragraphs 24-27. See also *Österreichischer Rundfunk and Other*, paragraph 64; *Satakunnan Markkinapörssi and Satamedia*, paragraphs 35-37; Case C-524/06 *Huber* [2008] ECR I-9705, paragraph 43; Case C-553/07 *Rijkeboer* [2009] ECR I-0000, paragraph 62; Case C-461/10 *Bonnier Audio and Others* [2012] ECR I-0000, paragraph 93; and *Volker und Markus Schecke and Eifert*, paragraphs 23, 55 and 56.

---

49 – Article 29 Working Party recalls that 'it is not necessary for information to be considered as personal data that it is contained in a structured database or file. Also information contained in free text in an electronic document may qualify as personal data …', see Opinion 4/2007, p. 8.

---

50 – There are search engines or search engine features specially targeting personal data, which, as such, can be identifiable because of their form (for example, social security numbers) or composition (strings of signs corresponding to names and surnames). See the Article 29 Working Party, Opinion 1/2008, p. 14. Such search engines may raise particular data protection issues that fall outside of the scope of this Opinion.

---

51 – However, so-called orphan pages without any links to other web pages remain inaccessible for the search engine.

---

52 – Web pages found by the crawler are stored in Google's index database which is sorted alphabetically by search term, with each index entry storing a list of documents in which the term appears and the location within the text where it occurs. Certain words like articles, pronouns and common adverbs or certain single digits and single letters are not indexed. See http://www.googleguide.com /google_works.html.

---

53 – These copies (so-called 'snapshots') of web pages stored in Google's cache only consist of HTML code, and not images which must be loaded from the original location. See Peguera, M., 'Copyright Issues Regarding Google Images and Google Cache', *Google and the Law*, pp. 169–202, at p. 174.

---

54 – Internet search engine service providers usually allow the webmasters to ask for the updating of the cache copy of the web page. Instructions on how to do this can be found on Google's Webmaster Tools page.

---

55 – It seems language versions of the Directive, other than the English, such as the French, German, Spanish, Swedish and Dutch, speak of an entity being 'responsible' for data processing, not of a controller. Some language versions, such as the Finnish and Polish use more neutral terms (in Finnish, '*rekisterinpitäjä*'; in Polish '*administrator danych*').

---

56 – *Lindqvist*, paragraph 68.

57– Article 29 Working Party, Opinion 1/2008, p.14, footnote 17. According to the Opinion, the role of users would typically be outside the scope of the Data Protection Directive as 'purely personal activity'. In my opinion this assumption is not tenable. Typically internet users also use search engines in activities that are not purely personal, such as use for purposes relating to work, studies, business or third-sector activities.

---

58 – The Article 29 Working Party gives in its Opinion 4/2007 numerous examples of the concept of and processing of personal data, including the controller, and it seems to me that in all of the examples presented this condition is fulfilled.

---

59 – Article 29 Working Party, Opinion 1/2010, p. 9.

---

60 – Ibid., p. 14.

---

61 – Dammann and Simitis (p. 120) observe that processing by automatic means must not only concern the support where the data is recorded (*Datenträger*), but also relate to the data in their semantic or substantive dimension. In my opinion it is crucial that personal data is according to the directive 'information', i.e. semantically relevant content.

---

62 – Article 29 Working Party, Opinion 1/2008, p. 14.

---

63 – *Lindqvist*, paragraph 27.

---

64 – *Satakunnan Markkinapörssi and Satamedia*, paragraph 37.

---

65 – Article 29 Working Party, Opinion 1/2010, pp. 4 and 9.

---

66 – Article 29 Working Party, Opinion 1/2008, p. 14.

---

67 – Article 29 Working Party, Opinion 1/2008, p. 14, however adds that the extent to which it has an obligation to remove or block personal data may depend on the general tort law and liability regulations

of the particular Member State. In some Member States national legislation provides ‘notice and take down’ procedures that the internet search engine service provider must follow in order to avoid liability.

---

68 – According to one author such filtering is done by Google in nearly all countries, for example in relation to infringements of intellectual property rights. Moreover, in the United States information critical to scientology has been filtered. In France and Germany Google is filtering search results relating to ‘Nazi memorabilia, Holocaust deniers, white supremacist and sites that make propaganda against the democractic constitutional order’. For further examples see Friedmann, D., ‘Paradoxes, Google and China: How Censorship can Harm and Intellectual Property can Harness Innovation’, *Google and the Law*,,p p. 303-327,at p. 307.

---

69 – See paragraph 41 above.

---

70 – First Report on the application of [ecommerce Directive 2000/31], COM(2003)702 final, p. 13, footnote 69 and Article 29 Working Party, Opinion 1/2008, p. 13, footnote 16.

---

71 – See paragraph 41 above.

---

72 – The capacity of a personal name to identify a natural person is context dependent. A common name may not individualise a person on the internet but surely, for example, within a school class. In computerised processing of personal data a person is usually assigned to a unique identifier in order to avoid confusion between two persons. Typical examples of such identifiers are social security numbers. See in this regard Article 29 Working Party, Opinion 4/2007, p. 13 and Opinion 1/2008, p. 9, footnote 11.

---

73 – It is interesting to note, however, that, in the context of data stored by government agencies, the European Court of Human Rights has held that ‘domestic law should notably ensure that such data are relevant and not excessive in relation to the purpose for which they are stored; and preserved in a from which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored’ (see *S. and Marper v. United Kingdom*, nos. 30562/04 and 30566/04, § 103, ECHR 2008; see also *Segerstedt-Wiberg and Others v. Sweden*, no. 62332/00, § 90, ECHR 2006-VII). However, the European Court of Human Rights has equally recognised, in the context of the Article 10 ECHR, right to freedom of expression, ‘the substantial contribution made by internet archives to preserving and making available news and information’ (*Times Newspapers Ltd v. the United Kingdom (nos. 1 and 2)*, nos. 3002/03 and 23676/03, § 45, ECHR 2009).

---

74 – See paragraph 41 above.

---

75 – Cf. Article 14 of the ecommerce Directive.

76– Article 29 Working Party, Opinion 1/2008, p. 14.

---

77 – This was the approach developed by the Court in *McB*, paragraphs 44 and 49..

---

78 – Joined Cases C-468/10 and C-469/10 *ASNEF and FECEMD* [2011] ECR I-0000, paragraphs 44–45. The European Court of Human Rights has noted that publication of personal data elsewhere ends the overriding interest relating to protection of confidentiality, see Aleksey *Ovchinnikov v. Russia*, no. 24061/04, § 49, 16 December 2010,.

---

79 – European Court of Human Rights: *Niemietz v. Germany*, 16 December 1992, § 29, Series A no. 251-B; *Amann v. Switzerland* [GC], no. 27798/95, § 65, ECHR 2000-II; and *Rotaru v. Romania* [GC], no. 28341/95, § 43, ECHR 2000 V.

---

80 – Paragraph 52 of the judgment.

---

81 – In contrast, the European Court of Human Rights has declined from giving a definition of private life in positive terms. According to that Court, the notion of private life is a broad one, which is not susceptible to exhaustive definition (see *Costello-Roberts v. the United Kingdom*, 25 March 1993, § 36, Series A no. 247-C).

---

82 – On positive obligations on the State to act to protect privacy, when it is being breached by private sector actors, and the need to balance any such obligation on the right to freedom of expression of the latter, see for example *Von Hannover v. Germany*, no. 59320/00, ECHR 2004-VI, and *Ageyevy v. Russia*, no. 7075/10, 18 April 2013.

---

83 – European Court of Human Rights: *Handyside v. the United Kingdom*, 7 December 1976, § 49, Series A no. 24; *Müller and Others v. Switzerland*, 24 May 1988, § 33, Series A no. 133; *Vogt v. Germany*, 26 September 1995, § 52, Series A no. 323; and *Guja v. Moldova* [GC], no. 14277/04, § 69, ECHR 2008. See also Case C-274/99 P *Connolly* v *Commission* [2001] ECR I-1611, paragraph 39 and Opinion of Advocate General Kokott in *Satakunnan Markkinapörssi and Satamedia*, point 38.

---

84 – Case C-360/10 *SABAM* v *Netlog* [2012] ECR I-0000, paragraph 48.

---

85 – United Nations, Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue (Document A/HRC/17/27), of 16 May 2011.

---

86 – *Satakunnan Markkinapörssi and Satamedia*, paragraph 60.

---

87 – It should be recalled here that the journalism exception in Article 9 of the Directive applies ‘not only to media undertakings but also to every person engaged in journalism’, see *Satakunnan Markkinapörssi and Satamedia*, paragraph 58.

---

88 – European Court of Human Rights: *Times Newspapers Ltd (nos. 1 and 2)*, § 45.

---

89 – Case C-70/10 *Scarlet Extended* [2011] ECR I-0000, paragraph 46, and *SABAM* v *Netlog*, paragraph 44

---

90 – See also Joined Cases C-317/08 to C-320/08 *Alassini and Others* [2010] ECR I-221, paragraph 63, where it was held that 'it is settled case-law that fundamental rights do not constitute unfettered prerogatives and may be restricted, provided that the restrictions in fact correspond to objectives of general interest pursued by the measure in question and that they do not involve, with regard to the objectives pursued, a disproportionate and intolerable interference which infringes upon the very substance of the rights guaranteed (see, to that effect, Case C-28/05 *Doktor and Others* [2006] ECR I-5431, paragraph 75 and the case-law cited, and the judgment of the European Court of Human Rights in *Fogarty v. the United Kingdom*, no. 37112/97, § 33, ECHR 2001-XI (extracts))'.

---

91 – Paragraph 50 of the judgment.

---

92 – Cited above.

---

93 – On the right to receive information, see European Court of Human Rights, *Observer and Guardian v. the United Kingdom*, 26 November 1991, § 60, Series A no. 216, and Timpul Info-Magazin *and Anghel v. Moldova*, no. 42864/05, § 34, 27 November 2007.

---

94 – Thomas Bowdler (1754–1825) published a sanitised version of William Shakespeare's works which intended to be more appropriate for 19th century women and children than the original.

---

95 – *SABAM* v *Netlog*, paragraphs 45-47.

---

96 – My Opinion in *L'Oréal and Others*, point 155.

---

97 – *SABAM* v *Netlog*, paragraphs 48 and 50.

---

98 – Article 29 Working Party, Opinion 1/2008,p p. 14-15.